In the Claims

Claims pending

- At time of the Action: Claims 1-39.
- After this Response: Claims 1, 2, 4, 7-11, 13, 14, 16, 19-25, 28, 29, 31 and 34-39.

Currently Amended Claims: Claims 1, 13, 23 and 28.

Currently Canceled claims: Claims 3, 5, 6, 12, 15, 17, 18, 26, 27, 30, 32 and 33.

1. (**Currently Amended**) A method comprising:

generating an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve, wherein the isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof;

publishing a public key corresponding to the isogeny;

encrypting a message using a encryption key corresponding to the isogeny; and

decrypting the encrypted message using a decryption key corresponding to the isogeny, wherein the decrypting is performed by bilinear pairing and wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing; and

using a trace map to shorten points on an Abelian variety.

2. (**Original**) A method as recited by claim 1, wherein at least one of the encryption key or the decryption key is a private key, the private key being a dual isogeny of the isogeny.

3. (**Canceled**)

4. (**Original**) A method as recited by claim 1, wherein the generating maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves.

5. (**Canceled**)

6. (**Canceled**)

7. (**Original**) A method as recited by claim 1, wherein the method is applied using Abelian varieties.

8. (**Original**) A method as recited by claim 1, wherein the method signs the message.

9. (**Original**) A method as recited by claim 1, wherein the method provides identity based encryption.

10. (**Original**) A method as recited by claim 1, further comprising composing a plurality of modular isogenies to provide the isogeny without revealing any intermediate curves.

11. (**Original**) A method as recited by claim 1, further comprising using a trace map down to a base field to shorten points on an elliptic curve mapped by the isogeny.

12. (**Canceled**)

13. (**Currently Amended**) A method comprising:

publishing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve, wherein the isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof; and

decrypting an encrypted message using a decryption key corresponding to the isogeny, wherein the decryption is performed by

bilinear pairing and wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing.

14. (**Original**) A method as recited by claim 13, wherein the decryption key is a dual isogeny of the isogeny.

15. (**Canceled**)

16. (**Original**) A method as recited by claim 13, wherein the isogeny maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves.

17. (**Canceled**)

18. (**Canceled**)

19. (**Original**) A method as recited by claim 13, wherein the method is applied using Abelian varieties.

20. (**Original**) A method as recited by claim 13, wherein the method signs the message.

21. (**Original**) A method as recited by claim 13, wherein the method provides identity based encryption.

22. (**Original**) A method as recited by claim 13, further comprising using a trace map down to a base field to shorten points on an elliptic curve mapped by the isogeny.

23. (**Currently Amended**) A system comprising:

a first processor;

a first system memory coupled to the first processor, the first system memory storing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve;

a second processor;

a second system memory coupled to the second processor, the second system memory storing an encrypted message and a decryption key corresponding to the isogeny to decrypt the encrypted message, wherein the decryption is performed by bilinear pairing and wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing,

wherein the encrypted message is encrypted using an encryption key.

24. (**Original**) A system as recited by claim 23, wherein at least one of the encryption key or the decryption key is a private key, the private key being a dual isogeny of the isogeny.

25. (**Original**) A system as recited by claim 23, wherein the isogeny maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves.

26. (**Canceled**)

27. (**Canceled**)

28. (**Currently Amended**) One or more computer-readable media having instructions stored thereon that, when executed, direct a machine to perform acts comprising:

publishing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve, wherein the isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof; and

decrypting an encrypted message using a decryption key corresponding to the isogeny, wherein the decrypting is performed by

bilinear pairing and wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing.

29. (**Original**) One or more computer-readable media as recited by claim 28, wherein the decryption key is a private key, the private key being a dual isogeny of the isogeny.

30. (**Canceled**)

31. (**Original**) One or more computer-readable media as recited by claim 28, wherein the isogeny maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves.

32. (**Canceled**)

33. (**Canceled**)

34. (**Original**) One or more computer-readable media as recited by claim 28, wherein the acts are applied using Abelian varieties.

35. (**Original**) One or more computer-readable media as recited by claim 28, wherein the acts further comprise using a trace map down to a base field to shorten points on an elliptic curve mapped by the isogeny.

36. (**Original**) One or more computer-readable media as recited by claim 28, wherein the acts further comprise composing a plurality of modular isogenies to provide the isogeny without revealing any intermediate curves.

37. (**Original**) One or more computer-readable media as recited by claim 28, wherein the acts further comprise using a trace map to shorten points on an Abelian variety.

38. (**Original**) One or more computer-readable media as recited by claim 28, wherein the acts sign the message.

39. (**Original**) One or more computer-readable media as recited by claim 28, wherein the acts provide identity based encryption.